Engineering Cryptographic Software

Background

Radboud University, Nijmegen, The Netherlands

Winter 2024/25

About me

- E-Mail: peter@cryptojedi.org

About me

- E-Mail: peter@cryptojedi.org
- Professor at Radboud University (Nijmegen, NL)
- Since 2020 part time

About me

- E-Mail: peter@cryptojedi.org
- Professor at Radboud University (Nijmegen, NL)
- Since 2020 part time
- Scientific Director at Max Planck Institute for Security and Privacy (MPI-SP)

About MPI-SP

- One of more than 80 Max Planck Institutes
- Founded in 2019
- Located in Bochum, Germany
- Today: 6 directors + 5 faculty
- Goal: 6 directors + 12 faculty
- Internship and Ph.D. programs within CS@MaxPlanck; see https://www.cis.mpg.de/

About this course

- Taught at Radboud University since 2014
- See https://cryptojedi.org/peter/teaching/engineering-crypto-software-2025.shtml
- Lectures Friday 8am CET in Zoom
- Lectures from Nov. 7 until Dec. 19 (7 lectures)
- Tutors: Romarick Mbah and Melchisedech Mbeng

About this course

- Taught at Radboud University since 2014
- See https://cryptojedi.org/peter/teaching/engineering-crypto-software-2025.shtml
- Lectures Friday 8am CET in Zoom
- Lectures from Nov. 7 until Dec. 19 (7 lectures)
- Tutors: Romarick Mbah and Melchisedech Mbeng
- No exam
- Programming assignment on embedded CPU
- Work **in groups of 2**
- Assignment grade = course grade
- Deadline for assignment: December 21
- Resit deadline for assignment: January 25

About this course

- Taught at Radboud University since 2014
- See https://cryptojedi.org/peter/teaching/engineering-crypto-software-2025.shtml
- Lectures Friday 8am CET in Zoom
- Lectures from Nov. 7 until Dec. 19 (7 lectures)
- Tutors: Romarick Mbah and Melchisedech Mbeng
- No exam
- Programming assignment on embedded CPU
- Work **in groups of 2**
- Assignment grade = course grade
- Deadline for assignment: December 21
- Resit deadline for assignment: January 25
- Recommended prerequesite knowledge:
  - C programming
  - Course on cryptology